University of Bahrain
College of Information Technology
Department of Computer Science
Second Semester, 2013-2014
ITCS412 (Cryptography and Network Security)

Test I

Duration: One Hour

Time: 3:00PM - 4:00PM

STUDENT NAME	
STUDENT ID #	
SECTION #	9:00 → (1) 12:00 → 2

NOTE: THERE ARE SIX **(6) PAGES** IN THIS TEST
ONLY ONE SOLUTION WILL BE CONSIDERED FOR EACH QUESTION

Part #	MARKS	COMMENTS
1	10	
2	16	
3	14	
TOTAL	40	

Part 1:

Answer the following questions by clearly circling *the most appropriate* answer (1 point *each*)

1. Eavesdropping is what type of attack?
   a. Active
   b. Passive
   c. Aggressive
   d. Masquerading

2. What is the inverse of confidentiality, integrity, and availability (C.I.A.) in risk management?
   a. misuse, exposure, destruction
   b. authorization, non-repudiation, integrity
   c. disclosure, alteration, destruction
   d. confidentiality, integrity, availability

3. What type of cryptographic attack enables an attacker to discover the cryptographic key by selecting a series of plaintext and corresponding ciphertext?
   a. Purchase-key attack
   b. Chosen plaintext attack
   c. Known plaintext attack
   d. Chosen-key attack

4. 3DES (Tripple Data Encryption Standard) is based on which of the following?
   a. Hashing algorithm
   b. Symmetric key-based algorithm
   c. Asymmetric key-based algorithm
   d. None of these

5. What characteristic of Digital Encryption Standard (DES) used in Electronic Code Book (ECB) mode makes it unsuitable for long messages?
   a. Block fragmentation causes message cipher instability.
   b. Weak keys will produce symmetrical message holes.
   c. Each message block produces a single cipher text block.
   d. Repeated message blocks produce repeated cipher text blocks.

6. What is the main component in DES that is responsible for diffusion

   a. The S-box
   b. The subkeys
   c. The swap operation
   d. The initial permutation (IP)

7. DES creates 16 subkeys from a key. Which of the following can be considered a weak key:

   a. Weak keys: keys with more ones than zeros
   b. Weak keys: keys with more zeros than ones.
   c. Weak keys: keys that make all subkeys to be different.
   d. Weak keys: keys make the same subkey to be generated in more than one round.

8. If by $E_K( )$ we denote the encryption function of a block cipher with a key K, and if the mode of operation is $C_i = E_k(P_i \; XOR \; C_{i-1})$ then the mode of operation is:

   a. ECB (Electronic Code book)
   b. CBC (Cipher Block Chaining)
   c. CFB (Cipher FeedBack)
   d. OFB (Output FeedBack)
   e. CTR (Counter)

9. In AES, the first and the last round begin with the following reversible part:

   a. MixColumns
   b. AddRoundKey
   c. ShiftRows
   d. Substitute bytes
   e. KeyExpand

10. In DES, if a small number of encodings give back the plaintext, what is likely the cause?
    (DES have 16 rounds with 16 subkeys, subscript indicate round subkey)

    a. $k_1=k_3$, $k_2=k_4$, $k_5=k_7$, $k_6=k_8$,..
    b. $k_2=k_1+1$, $k_3=k_2+1$, $k_4=k_3+1$,...
    c. $k_1..k_8$, $k_9=k_8$, $k_{10}=k_7$, $k_{11}=k_6$,.. $k_{16}=k_1$
    d. k_1=all bits are 1's, k_8=all bits are 1's, k_{16}=all bits are 1's, remaining subkeys are all zeros.

Part 2:

1. Define each of the following attacks: [4 points]

   i. What is the "**traffic analysis**"?

   ii. What is a "**masquerade**"?

   iii. What is a "**replay**"?

   iv. What is a "**denial of service**"?

2. Explain what is "One-time pad" [2 points]

3. Construct a table for the Playfair Cipher with the keyword EFFECTIVENESS? [3 points]

   Then encrypt the phrase: "EXAMFO"

4. Assume the following **monoalphabetic** cipher where it uses a keyword from which the cipher sequence can be generated. For example, using the keyword, *MARVEL*, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

   Plain : a b c d e f g h i j k l m n o p q r s t u v w x y z

   Cipher : M A R V E L b c d f g h i j K n o p q s t u w x y z

Now, given the following keyword: ***Partime*** , generate the sequence of cipher letters using the above key word and use it to encrypt the word ***usb***. [3 points]

5. Substitution ciphers. [2 points]
   a. Monoalphabetic substitution cipher is not secure. Why?

   b. Playfair requires a double letter frequency table to break the algorithm. If a new algorithm uses triple letter substitution, what would be the frequency table size required to break the algorithm? (for 26 English letters)

6. In the ciphertext obtained using Vigenere cipher, a four character sequence "GMBH" appears at positions 24, 57, and 101. Based on this information, the most period of Vigenere cipher is? (Hint: 3 or 4 or 11 or 13 or 17) [2 points]

Part 3:

7. What is the Double version of the 56-bit DES, and why is it much less secure than the expected 112-bit DES? (Not enough to give just the name of it.) [3 points]

8. About how many more times does a brute force key search take against a 106-bit key than against a 56-bit key? [2 points]

9. Assume we are using **EDE** with the 3 keys: K1 and K2, K3. [2 points]
Evaluate the cryptographic strength of following schemes by writing either *weak* or *strong* .

i. Using 1 key:
$$m \rightarrow E_{k1} \rightarrow D_{k1} \rightarrow E_{k1} \rightarrow c$$

ii. Using 2 keys:
$$m \rightarrow E_{k1} \rightarrow D_{k2} \rightarrow E_{k2} \rightarrow c$$

iii. Using 2 keys:
$$m \rightarrow E_{k1} \rightarrow D_{k2} \rightarrow E_{k1} \rightarrow c$$

iv. Using 3 keys:
$$m \rightarrow E_{k1} \rightarrow D_{k2} \rightarrow E_{k3} \rightarrow c$$

10. AES and DES design issues [2 points]
For each of the following elements of DES, indicate the comparable element in AES.

i. XOR of subkey material with the input to the f function.

ii. XOR of the *f* function output with the left half of the block.

iii. The *f* function

iv. Permutation p

11. Ben has invented a Feistel cipher that is similar to DES but has only 3 rounds with the same subkey used in each round and an *F* function which performs the following:

F(*m*, *k*) = *k* xor *m*

Convince Ben that the resulting cipher is not secure. [5 points]